PRIVACY IS NOT A ROSE

September 23, 2007

Two famous sayings in English are "A rose by any other name would smell as sweet" and "A rose is a rose is a rose." Both Shakespeare and Gertrude Stein believed that there was an identical essence of rose-ness, whatever it was called and wherever it was located.

But the concept of privacy is not a rose by any name. Privacy is a concept that is seemingly universal, but what is private and under what circumstances differs widely between peoples and over time. Let me begin by recounting several personal experiences.

Example 1
When I was part of the National Archives appraisal project on the records of the FBI, we project archivists were absolutely barred from seeing income tax return information in the files. The agents who looked at the files before handing them to us would put a brown paper bag over any tax return in the file, and we would simply note on our review sheet that a tax document was included. In Sweden, by contrast, personal income tax information is open to the general public—immediately.

Example 2
On a visit to Korea I was riding in a car with the then-director of the National Archives of Korea and his driver. In the midst of a general discussion, the director asked me, "Are you a Christian?" I mumbled something about being raised a Christian. This question is perfectly acceptable in his culture and mine today. By contrast, in countries and eras ranging from Nazi-period Poland to Bosnia during the 1990s, not to mention the period of the Inquisition in Europe, information on the religious persuasion of an individual was a private matter of the gravest consequence.

These examples show how differently national or ethnic groups conceive of what is private and what is not. Even countries that have many common ideas, such as the U.S. and Sweden, end up in quite different positions on privacy.

So is there anything one can say about an international norm on privacy? Let's look at three international statements from three different eras: the 1948 Universal Declaration of Human Rights, the 1980 OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, and the 1997 Principles for the Protection and Promotion of Human Rights Through Action to Combat Impunity by the United Nations Commission on Human Rights.

Universal Declaration of Human Rights

The first place to look is the Universal Declaration on Human Rights, adopted by the new United Nations in 1948. A bit of history may be helpful. The Universal Declaration was written against the background of the horrors of World War II. The UN Charter mandated a Commission on Human Rights, and the UN's Economic and Social Council charged the Commission to come up with a recommendation and report "regarding . . . an international bill of rights." The Commission, chaired by Eleanor Roosevelt, worked for two years on a "Universal Declaration" (the Commission specifically wanted it to be a universal and not just a UN Declaration). The final version reflected the contributions of the 58 countries that made up the new United Nations.

Article 12 of the Declaration reads:

> No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks.

The background to Article 12 and the positions taken by the nations involved during its drafting are particularly interesting in light of the subsequent histories of the countries. The

basic language came from the Latin American countries that, at the same time as the Declaration was being drafted, were drafting the Organization of American States' American Declaration of the Rights and Duties of Man, also known as the Bogotá Declaration. The Bogotá Declaration, adopted six months before the Universal Declaration, stated, "Every person has the right to the protection of the law against abusive attacks upon his honor, his reputation, and his private and family life" and "Every person has the right to the inviolability and transmission of his correspondence."

In addition to using the drafts of the Bogotá document, the drafting committee for the Universal Declaration assembled copies of national constitutions and drew from their language.

For example, the constitution of Argentina declared:

"The domicile is inviolable, as also epistolary correspondence and private papers."

The Bolivian constitution said:

"Every house is an inviolable asylum" and "epistolary correspondence and private papers are inviolable."

Yugoslavia's read:

"The dwelling is inviolable" and "the privacy of letters and other means of communication is inviolable."

Similar phrases were found in the constitutions of Egypt, Iraq, Lebanon, Belgium, Denmark, and Luxembourg.

As the drafting got underway, the U.S. proposed a text reading:

"No one shall be subjected to arbitrary or unauthorized searches of his person, home, papers and effects, or to unreasonable interference with his person, home, family, relations with others, reputation, privacy, activities or property. The secrecy of correspondence shall be respected."

Panama suggested:

"Freedom from unreasonable interference with his person, home, reputation, privacy, activities, and property is the right of everyone. The State has the duty to protect this freedom."

The Chinese delegation proposed:

"No one shall be subjected to unreasonable interference with his privacy, family, home, correspondence or reputation."

And the Soviet Union offered:

"No one shall be subjected to arbitrary interference with his privacy, family, home, correspondence, honor and reputation."

During the debate over the Article, a delegate from the Philippines said that reputation needed to be protected, noting, "There were parts of the world where the former practices of Nazi Germany and Japan were being carried out. Reputations were ruined beyond repair by systematic defamation in the press and by other methods. Some safeguard against such attacks should be included."

Notice that in these drafts, privacy, reputation and correspondence are all mentioned, as if they are separate but related issues. Notice, too, that in all these comments, no definitions of privacy are offered. In an extremely detailed study of the drafting of the Declaration, Johannes Morsink[1] found no evidence of an attempt to define privacy. Rather like U.S. Supreme Court Justice Potter Stewart, who in 1964 famously said of pornography, "I know it

[1] Johannes Morsink, The Universal Declaration of Human Rights: Origins, Drafting & Intent. Philadelphia: University of Pennsylvania Press, 1999. See especially Chapter 4, sections 1 and 2, for a discussion of Article 12. This discussion is based on Morsink's analysis.

when I see it," the drafters appear to have thought that privacy as a concept was obvious. While the Nazi *government's* intrusion into privacy clearly forms the background to the development of the attitudes reflected in Article 12, the final language it does not exclude the intrusion by one *citizen* upon the privacy of another and, in fact, specifically requires the state to protect the citizens, one from another. The inclusion of the word "correspondence" in the Article is a specific archival link.

Although the drafting was done decades before the concept of "information" (as in "freedom of information") gained currency, the formulation of Article 12 prefigures the battles that were to take place later between those who support greater government openness and those who fear the exposure of the private lives of citizens though the greater access to government records. The inclusion of the word "arbitrary" in Article was inserted to signal that, if legally warranted, some invasions of privacy and correspondence could be made. The delegate from Saudi Arabia explained, "The right of every individual to be free from State interference in his private life must be regarded as sacred as long as that right was not used as a cloak for activities which were essentially detrimental to the general good, or which endangered its general welfare and security." So it was clear to the drafters that a government would hold at least some information that an individual would consider private. On the other hand, while the Declaration specified "everyone has the right to take part in the government of his country,"[2] it said nothing at all about a right to information about what the government was doing.

In 1976 a U.N. Covenant on Civil and Political Rights was adopted to further define the basic rights of individuals and nations.[3] Its Article 17, however, simply reiterates the Declaration.

In sum, the Universal Declaration and the subsequent Covenant do not get us very far towards an understanding of what is privacy for information found in the records of government (or, for that matter, privacy in the records of other institutions). The only clarity is that the personal correspondence of an individual, in the possession of that individual, should generally be protected from intrusion and not made public unless the person chooses to do so.

OECD Guidelines and the 1980s

During the late 1970s, the rapid adoption of computers in government agencies and private businesses led to a series of studies and recommendations on data protection. The Organisation for Economic Co-Operation and Development, a group of 30 member countries with 70 current non-member partner countries, was established in 1961. It serves as a major international economic think tank, and in the late 1970s it commissioned a group of experts to develop guidelines on transborder flow of data. The guidelines were adopted in 1980, with the OCED noting in the preface "that, although national laws and policies may differ, Member countries have a common interest in protecting privacy and individual liberties and in reconciling fundamental but competing values such as privacy and the free flow of information."[4] The Annex to the Guidelines defines "personal data" as "any information relating to an identified or identifiable individual (data subject)." And it specifically points out that the Guidelines apply to data in both the public and private sectors.

The OECD Guidelines were enormously influential. Nevertheless, they were aimed at the risk that domestic legislation, such as the data protection acts and privacy acts that were being enacted Europe and North America during the 1970s, would harm the flow of information necessary for commerce. By 1981 the United Nations Human Rights Commission's Sub-Commission on discrimination and minorities was studying "guidelines for computerized personal files, particularly as they affected the privacy of the individual."[5] This draft apparently was revised throughout the 1980s, and in 1991 the UN General Assembly adopted "guidelines for the regulation of computerized personal data files."[6] These guidelines do not

---

[2] Article 21
[3] The United States ratified the Covenant in 1992.
[4] Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data, 23 September 1980 – C(80)58/Final. http://webdomino1.oecd.org/horizontal/oecdacts.nsf/linkto/C(80)58 (accessed 2007-09-23).
[5] E/CN.4/1512
[6] E/CN.4/Sub.2/1988/22 and UN General Assembly resolution 44/132, 5 December 1989, "Guidelines for the regulation of computerized personal data files."

offer a definition of privacy or private information, simply calling it "information about persons" or "personal data."

Also during the decade of the 1980s, Interpol, the International Criminal Police Organisation, became involved in the question of privacy and data protection. During the process of revising the Headquarters agreement for Interpol, the UN General Assembly mandated the creation of an independent body to monitor the implementation of Interpol's data protection practices. Interpol then adopted a formal statement of its compliance with UN Guidelines on Data protection. Interpol noted, however, that the protection of the data it held that was sent to Interpol by national polices authorities was the responsibility of the sender.[7]

Finally, in the late 1980s UNESCO funded a study by the International Council on Archives on archival appraisal of records containing personal information. In that study, personal information was defined as "any information about an identifiable individual that is recorded in any format." While that is surely true, it leaves open the question of what of that information should be accorded privacy protection and, indeed, what is privacy in an archival context.[8]

Joinet Principles

A third large international step in stating a privacy right comes with the adoption of the Principles for the Protection and Promotion of Human Rights Through Action to Combat Impunity by the United Nations Commission on Human Rights.[9] Distinguished French legal scholar Louis Joinet developed the principles, which included five principles on the "preservation of and access to archives bearing witness to violations." The Joinet principles, adopted in 1997, were revised by American University law professor Diane Orentlicher in 2005.[10]

The Principles first obligate a State "to preserve archives and other evidence concerning violations of human rights and humanitarian law and to facilitate knowledge of those violations."[11] The Principles then go on to address the tension between access to archives to combat impunity and privacy for victims and other individuals (I read Joinet/Orentlicher to exclude from the "other individuals" category those persons who are implicated in human rights violations). The Principles posit a set of categories for access, based on the relationship of the person to the information sought. They are:

1. Victims and their relatives get access to records that would assist them in rights claims.
2. Persons implicated get access for their legal defense.
3. Historical researchers gain access "subject to reasonable restrictions aimed at safeguarding the privacy and security of victims or other individuals."[12]
4. "Courts and non-judicial commissions of inquiry, as well as investigators reporting to them" get access to "relevant archives" but "in a manner that respect applicable privacy concerns, including in particular assurances of confidentiality provided to victims and other witnesses as a precondition of their testimony."[13]
5. Finally, the Principles introduce the balancing test between access and privacy for access to "the files of commissions of inquiry" by requiring that access "be balanced

---

[7] Souheil El Zein, "Reconciling Data Protection Regulations with the Requirements of Judicial and Police Co-Operation," 14 September 1999, 21st International Conference on Privacy and Data Protection, http://www.pcpd.org.hk/english/infocentre/files/elzein-paper.doc (accessed 2007-09-23).

[8] Terry Cook, "The Archival Appraisal of Records Containing Personal Information: A Ramp Study with Guidelines. UNESCO: April 1991, PGI-91/WS/3. I was a member of the "group of experts" whose deliberations formed the basis for the study.

[9] Various regional groupings of nations had developed statements on privacy, and the OAS had revised its Bogotá Declaration during the intervening years.

[10] "The Administration of Justice and the Human Rights of Detainees: Question of the impunity of perpetrators of human rights violations (civil and political). Revised final report prepared by Mr. Joinet pursuant to Sub-Commission decision 1996/119," United Nations Commission on Human Rights, Sub-Commission on Prevention of Discrimination and Protection of Minorities, E/CN.4/Sub.2/1997/20/Rev.1, 1997-10-02; updated by E/CN.4/2005/102, 18 February 2005, and E/CN.4/2005/102/Add.1, 8 February 2005.

[11] Principle 3

[12] Principle 15 covers points 1-3.

[13] Principle 16

> against the legitimate expectations of confidentiality of victims and other witnesses testifying on their behalf."[14] The Principles further warn that at the outset of the work of commissions of inquiry, the commissions "should clarify the conditions that will govern access to their documents, including conditions aimed at preventing disclosure of confidential information while facilitating public access to their archives."[15] Further, "information that might identify a witness who provided testimony pursuant to a promise of confidentially [sic] must be protected from disclosure."[16]

In addition, the Principles address "specific measures relating to archives containing names," defined as "information that makes it possible, directly or indirectly, to identify the individuals to whom they relate." They state that a person is entitled to know when his or her name appears "in State archives."[17]

What is not covered in the Principles is a definition of privacy. The caution about information provided with a promise of confidentiality is reasonably clear, although it is sometimes hard to identify in files exactly which statements are covered by an implied as opposed to explicit promise. However, does the mere appearance of someone's name in a file as someone who talked to a commission require protection?

The question of duration is also not covered. Understandably, the Principles (like the Universal Declaration) have a presentist orientation. But what happens when the records of such a commission are 30 years old? 50? 100? And here we return to the cultural distinction between a society that considers the actions of ancestors equal to the action of today's generations (many Asian countries, for example) and a society like the United States where the principle of "no privacy for the dead" is generally accepted. Still, by acknowledging that there are different categories of users and that they have different right of access, the Joinet/Orentlicher Principles are a major step forward in an international understanding of privacy, particularly in an archival context.

So as we look for future international norms of privacy in the context of information found in documents, what are the trends?

I think there are two. First, of course, is the impact of YouTube and its ilk. For better or worse, the public has come to understand over the past two decades that an enormous quantity of digital information on individuals is available on line, either for free or for fee. Even unauthorized disclosures of information or losses of quantities of personal information in digital form no longer makes much impact on the public. Most people have scary stories about someone learning something about us from electronic sources, but for the most part such revelations are greeted with a shrug. What <u>is</u> new, it seems to me, is the willingness of people to disclose personal information by posting it on YouTube and its competitors. The difference here appears to be who is releasing the information: I can put up a video showing myself in a compromising position, but another person or an institution must not.

A recent "Candorville" cartoon strip has a Federal agent visiting a man named Lemont. Lemont complains in the first panel, "This invasion of privacy is outrageous!" In the second and third panels he is raging on, "It's none of your business that I'm marrying the mother of my child. My life is none of your business. I demand to see the files you have on me! I demand to know how you got all that detailed information!" In the final panel the agent replies, "I read it on your blog."[18]

For years archivists have taken the position that if the information has previously been revealed by authorized means (that is, not by a leak or a paparazzi), it could be released by the archives. Does that mean, however, if the person has posted a video to YouTube and information corresponding to the video is in the police files, that the archives can release the document found in the police files?

---

[14] Principle 17
[15] Principle 8(f)
[16] Principle 10(d)
[17] Principle 17(b)
[18] Darrin Bell, Candorville," printed in *The Washington Post*, September 19, 2007, p. C10.

Computer scientists are now developing a theory used by philosophers. Called "contextual integrity," it argues that people do not need complete privacy; they need privacy within certain social norms. Helen Nissenbaum, a scholar at New York University, thinks there are four variables in the question of contextual integrity: the context of a flow of information, the capacities in which the individuals sending and receiving are acting, the type of information, and how the information is transmitted.[19] Computer scientists are now working to develop computer programs that will look at the context of information requested, such as medical data, and determine whether the requester is authorized to see it.[20]

The second trend is the increasing development of the archives of international organizations, particularly international courts with their extensive records of persons: defendants, victims, witnesses, and persons who worked for the courts. As these records become archives and as the research requests for access begin, the international organizations will have to make some difficult decisions on privacy.[21] Because international organizations are, by definition, organizations that represent all governments and to whose decisions all governments have input, the course these archives follow on access will represent a consensus on what privacy is and when and how records containing privacy information can be released. Whether this will be an extremely conservative position, closing records indefinitely, remains to be seen.

In the future, it just may be that privacy standards will start to harmonize. Certainly the work in the European Union to develop a common position on access to archives points in that direction. But until that time, the privacy rose in one country will not smell the same as the rose in another country. Privacy is not a rose.

---

[19] Helen Nissenbaum, "Privacy as Contextual Integrity," *Washington Law Review*, v. 79, February 4, 2004, pp. 101-139, http://crypto.stanford.edu/portia/papers/RevnissenbaumDTP31.pdf (accessed 2007-09-23). "Personal Data: The Logic of Privacy," *The Economist*, January 6, 2007, pp. 65-66.

[20] Barth, Adam, Anupam Datta, John C. Mitchell, and Helen Nissenbaum, "Privacy and Contextual Integrity: Framework and Applications," Proceedings of the IEEE Symposium on Security and Privacy, May 2006, http://www.nyu.edu/projects/nissenbaum/papers/ci.pdf (accessed 2007-09-23)

[21] See, for example, Trudy Huskamp Peterson, United States Institute of Peace Special Report 170 Temporary Courts, Permanent Records, available at http://www.usip.org/pubs/specialreports/sr170.html.